EMAKHAZENI LOCAL MUNICIPALITY

DATA MANAGEMENT POLICY

Approval

DOCUMENT:	**DATA MANAGEMENT POLICY**		
Copy Number:	**Master Copy**		
Compiled by:	Niall Carroll	**Reviewed by:**	
Compilation Date:	August 2013	**Review Date:**	
Version:	V 1.03	**Revision:**	
Distribution:	All	**Classification:**	
Document Release Approval		**Document Acceptance**	
Releasing Authority: Deputy Manager: ICT	ICT	**Acceptance Authority:**	Council
Date Released:		**Date Accepted:**	
	Signature:		**Signature:**

DOCUMENT CONTROL

0.1 Revision Record

Revision	Date	Change Record	Changed By
1st	April 2009	New ICT Policy – submitted to Council	N Carroll ICT
2nd	March 2013	Reviewed and updated	N Carroll ICT
3rd	August 2013	Re formatted layout	N Carroll ICT

0.2 Issue Control

This policy is issued by the Corporate Services Department on behalf of Emakhazeni Local Municipality, to whom any change requests or queries should be directed. The review life for this document is 12 months.

0.3 Distribution

Copy No.	Name	Title	Organisation
Master			
01			
02			

The MASTER for this document is held electronically and only signed copies are valid. An unsigned, printed document is not copy controlled and is to be used for information purposes ONLY, as it will not be automatically updated. It is therefore the responsibility of the reader to ensure that it is a currently valid copy.

Table of Contents

PURPOSE OF THE POLICY

The purpose of the policy is to define and accurately control all data generated or input on the network. Although some of this may have been covered earlier it is still relevant to discuss under this heading.

1. GENERATED AND INPUT DATA

1.1. All data that are input into any computer system using either a mouse, keyboard, microphone, scanner or any other input device is referred to as input data. This includes the data captured by scanner as part of the document management system that is planned for the future for this office and other government offices around the country. All such data are to be carefully captured and verified for correctness as to ensure that all information generated or derived from it is accurate and just.

1.2. Generated data is usually the result of captured or input data. This type of data is usually the sought after product when budgets are compiled and are dependent upon the input data. Both types of data should be protected by secure connections and firewalls and anti-virus software. Generated data may not be changed or altered unless the relevant input data was verified as captured incorrectly.

2. MANAGEMENT OF GENERATED AND INPUT DATA

2.1. All data is important to the municipality and should be verified as being correct before and during the capturing process and then also afterwards. This will ensure that data is correct and this will ensure that accurate data or information is generated.

2.2. All users should receive a specified amount of storage space on the file server where data can be kept that are work related under their own name. This directory or folder should be accessible to the user only and can contain all correspondence and work related information generated between him/her and the supervisor or municipality for whatever reason. It should however not contain any private files such as data or programs. The municipality's Head of the Department responsible for Information Technology should decide upon the size of the directory where users may create, modify and erase data pertaining to themselves and the work. It is the user's prerogative on what he/she saves in

this directory as long as private and personal information is kept from the server.

2.3. Along with user home directories all functions should receive a space on the file server where data specifically pertaining to that job function can be kept. Such directories should have the name of the relevant function such as Finance or Personnel or Stock Control depending upon the functions and be accessible to the members of that function only. Only one or two people in such a function should receive rights to delete files from the directory or folder but all should be able to create new files, change the content there-of, view all the files and be able to generate output. These directories must contain data only pertaining to the function and not individuals unless data is generated in the name of an individual but it is applicable to the whole function. No private or personal data or programs may be kept in this directory.

2.4. A general directory or Intranet must be setup to publish data relevant to the whole municipality such as circulars for jobs, functions and new policies or general feedback to staff. Such a directory should be updated regularly and should only contain information relevant to all members of the municipality and should not contain personal or private data or programs. An Intranet will provide the function of feedback and keep the members of the municipality informed of work related issues and policies as well as social events and gatherings.

2.5. All generated data must be kept and should be verified only by an official verifier or auditor for example financial data input, input data for stock control and personnel related data. Generated data is dependent upon captured data and is normally used in feedback given to management or the public. Plans are formulated around generated data and it should therefore be properly managed and administered. Inaccurate data can lead to public condemnation and loss of support by the community.

2.6. All data irrespective of the type is important and should be protected against disaster and illegal access and corruption. Corrupted data is of no use and will ensure that systems fail or cancel as a result. All data that is captured or input into any system should be stored in one location. Data that is generated should be stored in a different location and Write, Erase and Modify access should only be granted to verifiers and auditors and members of management that needs this information to be available to them. No other person should have such

access privileges or rights to the relevant directories or folders where such data is kept.

2.7. All data should be regularly backed up and it is advisable that data be kept for a period of at least 3 months off site for disaster recovery. A full backup should be done at least once per week with differential backups done daily to ensure that all data are properly backed up and that data can be restored when needed.

2.8. Data should not be stored in different locations but should be stored together to ensure easy access and backup of data. It would be senseless to have the same type of data such as expenditure for March in 10 different directories as opposed to have it in one directory. When data access strategies are compiled and implemented it should be understandable and easily available to those needing to access it and work with such data. Users should not be allowed to store such data in their own home directories but should be given a directory where to work and manipulate the relevant data they need to work with and share with other users.

2.9. Users that do store sensitive information on their home directories should be shown where to save it. Such data should then be transferred to a common directory or folder where all applicable users can work with it. Care should be taken that data are grouped together in other words financial information should be kept separately from personnel information and public relations information etc. It should be clearly defined where data is kept and access should be granted to those directories or folders only and not to data or information that is not necessary for the person to work with. This will combat confusion and lessen the occurrence of mistakes.

2.10. All data that is distributed must be authorized for distribution before it is sent out or published on an Internet or Intranet site or in printed press. Data that is published in the press or on the Internet must be published in accordance with government policy and laws governing the release of information on all levels of government as well as individuals.